

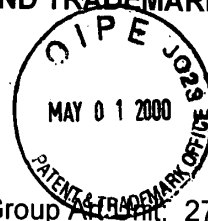
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of )

Masue SHIBA et al )

Serial No.: 09/487,483 )

Filed: January 19, 2000 )



Group Art Unit: 2766

Examiner: Not Assigned

For: ARITHMETIC METHOD AND APPARATUS  
AND CRYPTO PROCESSING APPARATUS

CLAIM FOR PRIORITY

Assistant Commissioner for Patents  
Washington, D.C. 20231

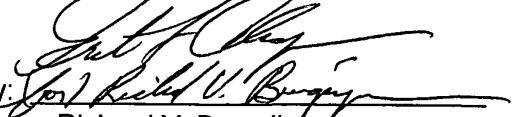
Sir:

Under the provisions of 35 U.S.C. § 119, Applicants hereby claim the benefit of the filing date of Japanese Patent Application Nos. 11-011989, filed on January 20, 1999 and 11-209831, filed on July 23, 1999, for the above-identified U.S. patent application.

In support of Applicants' claim for priority, filed herewith are certified copies of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,  
GARRETT & DUNNER, L.L.P.

By: 

Richard V. Burgujian

Reg. No. 31,744

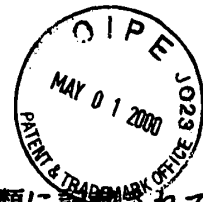
ERNEST F. CHAPMAN

Reg. No. 25,961

Dated: May 1, 2000  
RVB/FPD/sci  
Enclosure

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 1月20日

出 願 番 号

Application Number:

平成11年特許願第011989号

出 願 人

Applicant (s):

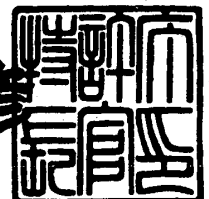
株式会社東芝

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 1月28日

特 許 庁 長 官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3001158

【書類名】 特許願

【整理番号】 A009807708

【提出日】 平成11年 1月20日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 7/00

【発明の名称】 演算装置及び暗号処理装置

【請求項の数】 7

【発明者】

【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

【氏名】 斯波 万恵

【発明者】

【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中工場内

【氏名】 川村 信一

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 演算装置及び暗号処理装置

【特許請求の範囲】

【請求項 1】 多倍長の積和演算装置であって、

整数型の単位乗算を実行する場合にはキャリーを伝搬させて単位乗算回路を動作させ、2の拡大体の単位乗算を実行する場合にはキャリーを伝搬させずに単位乗算回路を動作させるようにしたことを特徴とする演算装置。

【請求項 2】 少なくとも整数型の単位乗算回路を含んで構成される多倍長整数の積和演算装置であって、

前記整数型の単位乗算回路と論理的に隣接して配置された2の拡大体の単位乗算回路と、

前記整数型の単位乗算回路を使用するか、前記2の拡大体の単位乗算回路を使用するかを選択する選択手段と  
を備えたことを特徴とする演算装置。

【請求項 3】 少なくとも整数型の単位乗算回路を含んで構成される多倍長整数の積和演算装置であって、

整数型の単位乗算を実行するか、2の拡大体の単位乗算を実行するかの選択信号を前記整数型の単位乗算回路に出力する制御手段を備えとともに、

前記整数型の単位乗算回路は、多倍長の積和演算を実行する際に、整数型の単位乗算を実行すべき旨の選択信号を受けたときにはキャリーを伝播し、2の拡大体の単位乗算を実行すべき旨の選択信号を受けたときにはキャリー伝搬をしないキャリー伝搬制御手段を備え、

前記単位乗算回路におけるキャリー伝搬を制御することにより、整数型乗算と2の拡大体の乗算を切替可能に構成されたことを特徴とする演算装置。

【請求項 4】 請求項 3 の演算装置において、

前記キャリー伝搬制御手段は、前記選択信号とキャリーアウト信号を入力とするスイッチによって、1ビット毎の全加算器におけるキャリーの伝搬制御を行うことを特徴とする演算装置。

【請求項 5】 請求項 3 の演算装置において、

前記キャリー伝搬制御手段は、1ビット毎の全加算器における2入力a, bの排他的論理和の結果cを加算結果として出力するか、前記結果cと入力キャリーとの排他的論理和の結果dを加算結果として出力するかを切り替える選択手段からなることを特徴とする演算装置。

【請求項6】 請求項1乃至5のうち何れか1項に記載の演算装置において

前記整数型の乗算を実行する場合にはキャリーを伝搬させて加算を実行し、2の拡大体の乗算を実行する場合にはキャリーを伝搬させずに加算を実行する加算回路を備えたことを特徴とする演算装置。

【請求項7】 請求項1乃至6のうち何れか1項に記載の演算装置を備え、

前記演算装置による整数型の演算に基づく暗号化又は復号処理と、前記演算装置による2の拡大体の演算に基づく暗号化又は復号処理との双方を切替可能に構成されたことを特徴とする暗号処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は演算装置及び暗号処理装置、特に例えばICカードに実装される暗号処理用コプロセッサ等に用いるのに適した演算装置及び暗号処理装置に関するものである。

【0002】

【従来の技術】

公開鍵暗号のLSI実装においては、従来からRSA方式等の整数型の演算を行う暗号方式が主に採用されている。この方式では、桁数の大きい整数についての演算を行う必要があるため、ICカード等に応用する場合には専用コプロセッサが必要とされる。このような専用コプロセッサを実装して暗号処理の多倍長整数演算を実現させる方式については既に多数の実績がある。

【0003】

一方、近年整数型ではなく、2の拡大体( $GF(2^m)$ : Galois Field (ガロアフィールド))といわれる代数系の上で構成される暗号系、特

に2の拡大体の楕円暗号方式が注目されている。

【0004】

この2の拡大体演算を用いる暗号方式においても、RSA方式等の整数型の演算の方式の同様に、扱うビット数を160ビット以上と大きくとる必要がある。このため、ICカードのようなCPUの演算力が低い装置上でこれを実現しようとすると比較的処理時間がかかる。したがって、専用のハードウェア（コプロセッサ）を用いて高速化したいという要求がある。

【0005】

このようにRSA方式であっても、楕円暗号方式であっても、ICカード等において高速な暗号処理を実現させるためには専用の演算用コプロセッサを用意する必要がある。

【0006】

図10は暗号処理用のコプロセッサを含むICカード用LSIのブロック図である。

【0007】

同図に示す構成要素を含む専用LSIが例えばICカードに組み込まれる。このLSIにおいては、CPU、RAM、ROM、EEPROMが1チップに収容され、コプロセッサはRAM、演算部、制御部から構成される。コプロセッサはCPUの制御下にあつて多倍長のべき乗剰余演算や四則演算といった公開鍵暗号の基本演算に関しCPUを補助する。つまり、暗号の基本演算を行う部分は図10におけるコプロセッサであり、この部分がどのように構成されているかが問題となる。

【0008】

図11は図10に示すLSIにおけるコプロセッサ部分の構成例を示すブロック図である。

【0009】

RSA方式では整数型の演算が行われるため、このコプロセッサは図11に示すように整数型の乗算器として構成されている。

【0010】

一方、楕円暗号方式のLSIを作成する場合、その全体的な構成は図10に示すLSIと同様あるいはこれと類似する構成のものとなるが、コプロセッサ部分における演算は整数型の演算でなく、2の拡大体演算を行うコプロセッサを用意する必要がある。

## 【0011】

図12は多項式基底の2の拡大体演算を行うコプロセッサのハードウェア構成例を示すブロック図である。

## 【0012】

同図は、「楕円暗号のハードウェア実装、SCIS'98-10.1.C」にて発表された特殊な既約多項式を用いる円分体といわれる2の拡大体の一種の演算装置を示している。この演算装置は、2の拡大体上の加算、二乗、乗算及び逆元演算を実行できる構成を備えており、これによって楕円曲線上の点の演算に必要な2の拡大体の演算を実行する。このような演算装置をIC化すれば、図10のLSIに適用し得る2の拡大体演算用のコプロセッサになる。

## 【0013】

ここで、加算回路および二乗算回路はm個のEX-ORで構成され、乗算回路81は図13に示す回路構成で実現する。

## 【0014】

図13は円分体といわれる2の拡大体の乗算回路を示す図である。

## 【0015】

この乗算回路81は、mビットの入力レジスタA、Bを持ち多項式 $a(x)$ の係数を入力レジスタAに固定値として入力し、入力レジスタBからは多項式 $b(x)$ の係数を最上位ビットから1クロック毎にシフトしながら演算していく。同図におけるブロックDはフィードバックレジスタを構成するフリップフロップである。m回シフトした時点での各ブロックDの値が出力レジスタCに読み出され、 $a(x) * b(x)$ の演算結果となる。

## 【0016】

図11と図13夫々の回路を見比べてもわかるように、乗算と一口に言っても整数型乗算と多項式基底の2の拡大体乗算とでは、その乗算を実行するためのア



ーキテクチャーが全く異なる。したがって、従来は暗号方式毎にハードウェアを構成しようとする試みがなされてきた。

【0017】

【発明が解決しようとする課題】

上記したように、楕円暗号方式は現在注目されてはいるものの、現状ではRSA暗号方式が未だ主流であるため、楕円暗号方式を用いるICカードにおいてもRSA暗号にも対応させたいという要請が強い。

【0018】

ここで、従来の整数型の暗号と2の拡大体の暗号を同一ICカードに実装しようとした場合、上記した従来技術の延長ではそれぞれに対応するコプロセッサを搭載する必要が生じる。しかしながら、2つのコプロセッサを搭載したのでは、面積制約の大きいICカードにおいてそのチップ面積を圧迫するという問題が生じる。

【0019】

本発明は、このような実情を考慮してなされたもので、最小のアーキテクチャを追加するだけで整数型の演算に加えて2の拡大体上の演算をも実行できる演算装置及び暗号処理装置を提供することを目的とする。

【0020】

【課題を解決するための手段】

上記課題を解決するために、請求項1に対応する発明は、多倍長の積和演算装置であって、整数型の単位乗算を実行する場合にはキャリーを伝搬させて単位乗算回路を動作させ、2の拡大体の単位乗算を実行する場合にはキャリーを伝搬させずに単位乗算回路を動作させるようにした演算装置である。

【0021】

本発明はこのような手段を設けたので、最小のアーキテクチャを追加するだけで整数型の演算に加えて2の拡大体上の演算をも実行することができる。

【0022】

次に、請求項2に対応する発明は、少なくとも整数型の単位乗算回路を含んで構成される多倍長整数の積和演算装置であって、整数型の単位乗算回路と論理的

に隣接して配置された 2 の拡大体の単位乗算回路と、整数型の単位乗算回路を使用するか、2 の拡大体の単位乗算回路を使用するかを選択する選択手段とを備えた演算装置である。

【0023】

本発明はこのような手段を設けたので、2 の拡大体の単位乗算回路を追加するだけで整数型の乗算と 2 の拡大体の乗算の双方を実行することができる。

【0024】

次に、請求項 3 に対応する発明は、少なくとも整数型の単位乗算回路を含んで構成される多倍長整数の積和演算装置であって、整数型の単位乗算を実行するか、2 の拡大体の単位乗算を実行するかを選択信号を整数型の単位乗算回路に出力する制御手段を備えるとともに、整数型の単位乗算回路は、多倍長の積和演算を実行する際に、整数型の単位乗算を実行すべき旨の選択信号を受けたときにはキャリーを伝播し、2 の拡大体の単位乗算を実行すべき旨の選択信号を受けたときにはキャリー伝播をしないキャリー伝播制御手段を備え、単位乗算回路におけるキャリー伝播を制御することにより、整数型乗算と 2 の拡大体の乗算を切替可能に構成された演算装置である。

【0025】

本発明はこのような手段を設けたので、キャリー伝播制御手段を追加するだけで整数型の乗算と 2 の拡大体の乗算の双方を実行することができる。

【0026】

次に、請求項 4 に対応する発明は、請求項 3 の演算装置において、キャリー伝播制御手段は、選択信号とキャリーアウト信号を入力とするスイッチによって、1 ビット毎の全加算器におけるキャリーの伝播制御を行う演算装置である。

【0027】

本発明はこのような手段を設けたので、選択信号とキャリーアウト信号を入力とするスイッチにより請求項 3 に係る発明を実現させることができる。

【0028】

次に、請求項 5 に対応する発明は、請求項 3 の演算装置において、キャリー伝播制御手段は、1 ビット毎の全加算器における 2 入力 a, b の排他的論理和の結

果 c を加算結果として出力するか、結果 c と入力キャリーとの排他的論理和の結果 d を加算結果として出力するかを切り替える選択手段からなる演算装置である。

【0029】

本発明はこのような手段を設けたので、選択手段により請求項 3 に係る発明を実現させることができる。

【0030】

次に、請求項 6 に対応する発明は、請求項 1 ～ 5 の演算装置において、整数型の乗算を実行する場合にはキャリーを伝搬させて加算を実行し、2 の拡大体の乗算を実行する場合にはキャリーを伝搬させずに加算を実行する加算回路を備えた演算装置である。

【0031】

本発明はこのような手段を設けたので、積和演算における加算部分についても整数型の乗算と 2 の拡大体の乗算との双方を確実に実行することができる。

【0032】

次に、請求項 7 に対応する発明は、請求項 1 ～ 6 の何れかの演算装置を備え、演算装置による整数型の演算に基づく暗号化又は復号処理と、演算装置による 2 の拡大体の演算に基づく暗号化又は復号処理との双方を切替可能に構成された暗号処理装置である。

【0033】

本発明はこのような手段を設けたので、RSA 暗号等の整数型の演算に基づく暗号と、楕円曲線暗号等の 2 の拡大体の演算に基づく暗号の双方の処理を行うことができる。

【0034】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

(発明の第 1 の実施の形態)

図 1 は本発明の第 1 の実施形態に係る演算装置の構成例を示すブロック図である。

## 【0035】

コプロセッサ1として構成される本実施形態の演算装置は、整数型乗算及び2の拡大体乗算の双方の演算が可能な多倍長積和乗算装置であり、この乗算処理を仕方を制御することにより、加算、二乗あるいは逆元等の他の演算を実行するものである。また、本演算装置がLSI等に組み込まれることによってRSA暗号及び楕円暗号の双方が実現可能な暗号処理装置が構成される。ここで組込対象となるLSIは例えば図10に示すような装置である。

## 【0036】

このコプロセッサ1において演算部4は制御部5によってコントロールされ、演算途中のデータを格納するメモリ2から接続される32ビットのデータバス3からデータを入出力するようになっている。

## 【0037】

データバス3からの入力データはバッファZ、Y、Xに格納され、データバス3への出力データはバッファRに格納されるようになっている。

## 【0038】

入力データX及びYは乗算対象となるデータであり、このうちデータYは一度に多数桁の乗算となるのを回避するために所定桁毎に分割されたデータとして入力される。一方、データZは乗算を複数回に分けて実行するために生じる途中結果であり、これをXYの乗算結果に足し、さらにその和の結果にキャリーCと言われる桁上がり部分を足して1サイクルの乗算が終了する。その結果からキャリーを除いたデータRがバッファRを介してデータバス3に出力され、次のサイクルの演算にデータZとして使用される。このサイクルを複数回繰り返すことにより多倍長整数乗算あるいは2の拡大体乗算（厳密には後述のc'）の乗算が実現される。

## 【0039】

また、コプロセッサ1は、上記演算を実現するために、バッファX、Y、Z、Rの他、整数型乗算回路11、2の拡大体乗算回路12、セレクタ13、加算回路14、加算回路15、キャリー保持部16及び制御部5を備えている。

## 【0040】

整数型乗算回路 11 は、バッファ X 内のデータ X とバッファ Y 内のデータ Y とを整数型乗算し、その結果をセクタ 13 に出力する。

【0041】

2 の拡大体上乘算回路 12 は、バッファ X 内のデータ X とバッファ Y 内のデータ Y とにより 2 の拡大体上乘算の一部 (c') を実行し、その結果をセクタ 13 に出力する。

【0042】

セクタ 13 は、制御部 5 からの信号 S1 に従って、整数型乗算回路 11 又は 2 の拡大体上乘算回路 12 からの出力の何れかを加算回路 14 に出にする。

【0043】

加算回路 14 は全加算器からなり、バッファ Z 内のデータ Z とセクタ出力を加算して加算回路 15 に出力する。この加算回路 14 においては、整数型の加算と 2 の拡大体の加算との切替が制御信号 S1 に従って行われるようになっている。なお、この加算切替については後述する。

【0044】

加算回路 15 は、加算回路 14 の出力にキャリー保持部 16 に保持されたキャリー C を加算し上位 32 ビットを次のキャリー C としてキャリー保持部 16 に出力し、下位 8 ビットをこのサイクルの演算結果であるデータ R をとしてバッファ R に出力する。なお、加算回路 15 においても、制御信号 S1 により、整数型の加算と 2 の拡大体の加算との切替が行われるようになっている。

【0045】

キャリー保持部 16 は、加算回路 15 から出力されたキャリー C を保持し、次の演算サイクルにおいて保持したキャリー C を加算回路 15 に与える。

【0046】

制御部 5 は、整数演算制御部 21 と 2 の拡大体演算制御部 22 からなり、これらの何れかのコマンド群に従って演算部を制御する。このコマンド切り替えは、外部の CPU (例えば図 10 に示す CPU) からの指示によって行われる。

【0047】

整数演算制御部 21 は、演算部 4 を多倍長整数演算型の乗算器として動作する

ように制御するものである。このために、制御信号 S1 によりセクタ 13 が整数型単精度乗算器 11 の出力を加算回路 14 に出力するように制御するとともに、加算回路 14 及び 15 を整数型加算回路として動作するよう制御する。さらに、整数型乗算器として演算部 4 の動作を制御することで他の四則演算などの演算処理の実行する。

## 【0048】

また、2 の拡大体演算制御部 22 は、演算部 4 を 2 の拡大体乗算器として動作するように制御するものである。このために、制御信号 S1 によりセクタ 13 が 2 の拡大体単精度乗算器 11 の出力を加算回路 14 に出力するように制御するとともに、加算回路 14 及び 15 を 2 の拡大体加算回路として動作するよう制御する。さらに、2 の拡大体乗算器として演算部 4 の動作を制御することで加算、二乗算を実現する。

## 【0049】

なお、制御部 5 からは、上記した各処理を実現するため、制御信号 S2 を出力して各部を制御する。

## 【0050】

次に、以上のように構成された本実施形態における演算装置の動作について説明する。

## 【0051】

この演算装置（コプロセッサ 1）は、整数型の乗算装置に乗算回路 12，セクタ 13 等を組み込むことにより、2 の拡大体の乗算装置としての処理を実現可能とするものであるがある。ここで、2 の拡大体では、以下に示すように  $m-1$  次の多項式を  $m$  ビットのベクトル表現で表すことができる。

## 【0052】

$$\begin{aligned} a(x) &= a_{m-1}x^{(m-1)} + a_{m-2}x^{(m-2)} + \cdots + a_1x + a_0 \quad \dots (1) \\ &= [a_{m-1}, \dots, a_1, a_0] \end{aligned}$$

ここで、2 の拡大体の乗算は  $GF(2)$  上の  $m$  次の規約多項式  $g(x)$  をモジュラスとする剰余乗算である。また、2 の拡大体の二つの元  $a(x)$  と  $b(x)$  の積  $c(x)$  は、次のように定義されている。

## 【0053】

$$c(x) = a(x) * b(x) \bmod g(x) \quad \dots (2)$$

$$= \sum a_k * x^k * b(x) \bmod g(x)$$

2の拡大体の多項式の乗算は、図13に示すように乗数のサイクルシフトによるシフトレジスタを構成し、mサイクルシフト後の剰余多項式を乗算結果とするのが一般的であるが、本実施形態では整数型の暗号処理LSIで広く使われている多倍長の積和演算回路に若干の変更を加えて処理する。

## 【0054】

なお、制御部5からの制御信号S1により、コプロセッサ1が整数型の演算装置として動作するときには、同演算装置は多倍長積和演算回路として機能している。この多倍長積和演算回路において、制御信号S1による切替により、2の拡大体上乘算回路12において2の拡大体の乗算の一部分である(3)式が計算される。

## 【0055】

$$c'(x) = a(x) * b(x) \quad \dots (3)$$

なお、2の拡大体上乘算回路12では $c'$ を計算する段階においては(2)式における「 $c(x) \bmod g(x)$ 」の部分は計算されない。すなわち $c'$ 自体は、制御信号S1により乗算回路12及び加算回路14、15を切り替えるのみで、整数型乗算における2つの数の積と全く同様に演算される。

## 【0056】

なお、 $c'(x) = a(x) * b(x)$ においてmビットの乗数、被乗数は32ビットに分割されてメモリから読み出され、演算結果は32ビット毎にメモリに書き込まれる。この時、最終的な演算結果は2mビットとなる。

## 【0057】

整数型乗算回路11による整数演算と2の拡大体上乘算回路12による2の拡大体多項式演算の違いは、桁上がりの有無である。整数演算では足し算の論理式は

$$0 + 0 + \text{Carry} (=0) = 0, \text{Carry} = 0$$

$$1 + 0 + \text{Carry} (=0) = 1, \text{Carry} = 0$$

$$1 + 1 + \text{Carry} (= 0) = 0, \text{Carry} = 1$$

という様に下位ビットのキャリーを考慮した演算をしなければならないのに対し、2の拡大体の代数系においては、各ビットが多項式における次数の係数を示しているため異なる次数への桁上りを考慮しなくてもよい。

## 【0058】

このことに着目して本実施形態では整数型演算器（乗算器や加算器）において、キャリー伝播を許す通常モードと、キャリー伝播を実行しないモードを切り替えて使えるようにしているのである。ここでキャリー伝播を許さない（実行しない）モードは2の拡大体演算を行うのに用いられる。なお、キャリー伝播のモードを切り替えのために追加すべき回路は全体の回路規模に比べわずかである。

## 【0059】

図2は  $c'(x) = a(x) * b(x)$  を実現するための4\*4ビットの単位乗算の回路構成例を示す図である。

## 【0060】

同図の単位演算装置を8\*32ビット構成にしたものが図1における2の拡大体上乘算回路12である。なお、図2(b)の回路は同図(a)の回路の入力部分29を示すものである。

## 【0061】

一方、図3は整数型乗算を実現するための4\*4ビットの単位乗算の回路構成例を示す図である。

## 【0062】

同図の単位演算装置を8\*32ビット構成にしたものが図1における整数型乗算回路11である。なお、図3(a)に用いられる全加算器FAの構成は図3(c)に示され、さらに図3(c)に示す全加算器FAのキャリー31の構成が同図(d)に示されている。また、図3(b)の回路は同図(a)の回路の入力部分30を示すものである。

## 【0063】

本実施形態の演算装置では、2の拡大体上乘算回路12と整数型乗算回路11とが論理的に隣接して配置されており、制御部5の2の拡大体演算コマンドから



生成される制御信号 S 1 により整数型、2 の拡大体型のいずれかの乗算回路 1 1 , 1 2 が選択されて処理が行われる。

【0064】

セクタ 1 3 の出力は次段の加算回路 1 4 に入力される。ここで  $Z + (Y * X)$  加算回路 1 4 は 40 ビットのデータ ( $Y * X$ ) と 8 ビットのデータ Z の全加算器だが、ここでも前述の制御信号により各ビットの加算結果のキャリーを次段へ伝播しないスイッチを付加することにより 2 の拡大体の加算が実現される。

【0065】

図 4 は本実施形態におけるコプロセッサに用いられるキャリー制御機能付きの 4 ビットのリップルキャリー型全加算器の構成例を示すブロック図である。

【0066】

このような構成の全加算器を、40 ビットデータと 8 ビットデータとの加算が可能となるように拡張したものが図 1 の加算回路 1 4 である。

【0067】

また、図 4 の回路において、各全加算器 3 2 の間にはスイッチ 3 3 が設けられ、キャリーの伝搬を制御できるようになっている。

【0068】

図 5 は本実施形態の加算回路に用いられる全加算器及びキャリー制御スイッチの構成例を示す図である。

【0069】

この全加算器 3 2 及びスイッチ 3 3 は、1 ビット分のキャリー制御機能付き全加算器 4 2 を構成している。ここで、全加算器 3 2 は、図 3 (c) に示す全加算器 F A と同様に構成され、全加算器 3 2 内のキャリー 3 1 は図 3 (d) に示すキャリーと同様に構成されている。

【0070】

また、全加算器 3 2 間のキャリー伝搬ラインに設けられたスイッチ 3 3 は制御部 5 からの制御信号 S 1 によって制御され、整数型演算を行うときには接続され、2 の拡大体演算を行うときには遮断される。

【0071】

以上のように構成された加算回路 14 からの出力 ( $Z + (Y * X)$ ) は加算回路 15 に引き渡される。

## 【0072】

すなわち、演算ブロック最終段の  $C + Z + (Y * X)$  加算回路 15 によって、乗算結果の 40 ビットの下位 8 ビットがデータ R として出力され、上位 32 ビットが次のサイクルの  $Z + (Y * X)$  に足し込まれる。

## 【0073】

ここで、加算回路 15 は加算回路 14 と同様に、前述の制御信号 S1 により制御される図 4 に示すキャリー制御機能付き全加算器であるので、整数型では LSB に桁あわせをした全加算器として整数型加算が実行され、2 の拡大体演算では 2 の拡大体加算が実行される。

## 【0074】

加算回路 15 の出力データ R はデータバス 3 を介して一旦外部のメモリ 2 に出力され、再びデータ Z となってコプロセッサ 1 内に戻り整数型乗算若しくは 2 の拡大体上の乗算が継続され、必要なサイクル数だけ繰り返されて乗算結果が得られる。

## 【0075】

ここで 2 の拡大体の乗算コマンドでは、(2) 式の結果が得られるが、2 の拡大体乗算は (3) 式に示す定義通り、既約多項式  $g(x)$  をモジュラスとする剰余演算によって完結する。剰余演算は割り算の筆算同様、被除数の上位桁から商を立て現在の商と除数をかけたものから現在の被除数を引く (2 の拡大体では減算は加算と同じ) 処理を必要なサイクル数だけ繰り返せばよく、2 の拡大体の乗算コマンドと加算コマンドを実行することによって実現できる。2 の拡大体の二乗算は乗算と同じ処理で実現でき、逆元計算は、乗算と二乗算を相互に繰り返すことにより実現できる。

## 【0076】

一例として、2 の拡大体の加算コマンドに従って演算部 4 が 2 の拡大体の加算装置として機能する場合を説明する。

## 【0077】

2の拡大体上の加算は、通常多項式の加算と同じで、同じ次数の係数同士の足し算を行う。

【0078】

$$c(x) = a(x) + b(x) \quad \dots (4)$$

$$= [a_{m-1} + b_{m-1}, a_{m-2} + b_{m-2}, \dots, a_0 + b_0]$$

このとき、各次数の係数の和は  $0+0=1+1=0$ 、 $0+1=1+0=1$  となり、整数型加算のようにキャリーは発生しない。従って、2の拡大体での加算は、一般には  $m$  個の EX-OR で実装できることになる。

【0079】

整数型の乗算装置において加算は  $c = b + a * 1$  として扱えるので、本実施形態における2の拡大体の加算もこのアルゴリズムをそのまま利用し、 $c(x) = b(x) + a(x) * 1$  として実行する。この演算は加算回路14、15に図4の全加算器が用いられていることから、制御信号S1の切替で実現できる。

【0080】

また、制御信号S1による切替でコプロセッサ1は図11に示すコプロセッサと同様な機能を持つ回路となり、整数型演算も実現される。

【0081】

上述したように、本発明の実施の形態に係る演算装置は、整数型乗算装置に、整数型乗算の単位乗算装置と回路構成の似ている2の拡大体乗算の単位演算装置とを設け、整数型の乗算コマンドに2の拡大体演算コマンドとを追加し、2の拡大体演算コマンドから生成される制御信号により制御されるセレクタと、全加算器の各ビットのキャリーの伝播を制御するスイッチの追加するようにしたので、従来型のシフトレジスタによるシーケンシャルな2の拡大体の乗算装置を用いることなく整数および2の拡大体演算の両方を実行することができる。

【0082】

したがって、従来からある整数型の演算器への追加拡張機能として、ごく少ない命令と回路の追加することにより、多倍長の積和演算回路で2の拡大体の加算、乗算を実行することが可能な公開鍵暗号処理用アクセラレータを提供することができる。なお、本実施形態を実現するのに、必要な回路追加の量は全体の回路

規模に比べてわずかである。

【0083】

本実施形態の暗号処理装置によれば、暗号処理用コプロセッサとして、整数型のRSA方式に加え2の拡大体の楕円暗号方式も処理できる豊富な機能をもつLSIを特に実装面積を増大させることなく提供できる。したがって、ICカードのような実装可能面積の少ない装置において、RSA、楕円暗号の双方を処理できる暗復号装置を実現させることができる。

(変形例1)

本変形例では、図4に示す加算回路14、15を構成するキャリー制御機能付き全加算器について説明する。

【0084】

図6はキャリー制御機能付き全加算器の変形例を示す図である。

【0085】

このキャリー制御機能付き全加算器43は、スイッチ33と全加算器32から構成される点で図5の回路と共通する。しかし、図5の回路ではキャリー31の出力側にスイッチ33が設けられているのに対し、図6の回路ではキャリー31の入力側にスイッチ33が設けられている。

(変形例2)

本変形例では、更に他のキャリー制御機能付き全加算器について説明する。

【0086】

図7はキャリー制御機能付き全加算器の他の変形例を示す図である。

【0087】

このキャリー制御機能付き全加算器44は、加算結果の出力選択を制御することによりキャリー制御を行う。すなわちスイッチ33'はセレクタで構成され、このセレクタは制御信号S1に基づき、EXOR35又はEXOR36の出力を選択する。これを複数個連結したリップルキャリー型加算器は、制御信号S1によりキャリー伝播の有無を制御できる。

【0088】

図7の制御信号S1を2の拡大体演算コマンドによる制御信号とするとS1が

“1” のとき a と b の EXOR 35 の出力が演算結果となり、2 の拡大体の加算装置として機能し、S1 が “0” のとき全加算器の出力が演算結果となって整数型の加算装置として機能する。

(発明の第 2 の実施の形態)

図 8 は本発明の第 2 の実施形態に係る演算装置の構成例を示すブロック図であり、図 1 と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0089】

この演算装置であるコプロセッサ 1' は、図 1 における整数型乗算回路 11、2 の拡大体上乘算回路 12 及びセレクタ 13 に代えて乗算回路 41 を備える他、第 1 の実施形態と同様に構成されている。

【0090】

この乗算回路 41 は、制御部 5 からの制御信号 S1 によって整数型乗算と 2 の拡大体上乘算（(3) 式の c' のみ）を切り替えるようになっている。

【0091】

図 9 は本実施形態の乗算回路を実現するための 4 \* 4 ビットの単位乗算の回路構成例を示す図である。なお、現実の乗算回路 41 は、同図の単位演算装置を 8 \* 32 ビット構成にしたものである。また、図 9 (b) の回路は同図 (a) の回路の入力部分 29 を示すものである。

【0092】

この乗算回路 41 は、図 9 (a) に示すように、全加算器として図 5 に示すキャリー制御機能付き全加算器 42 を用いているので、制御信号 S1 に従ってキャリー伝搬の有無を制御できる。したがって、2 の拡大体演算コマンドによる整数型乗算と 2 の拡大体上乘算との切替が実現される。

【0093】

こうして本実施形態の演算装置では第 1 の実施形態と同様な動作が実現される。

【0094】

上述したように、本発明の実施の形態に係る演算装置及び暗号処理装置は、整

数型乗算回路 11, 2 の拡大体上乘算回路 12 及びセレクタ 13 に代えて乗算回路 41 を用いるようにし、一つの回路 41 で回路 11, 12 及び 13 の機能を実現するようにしたので、第 1 の実施形態と同様な効果が得られる他、より少ない回路追加で整数型乗算と 2 の拡大体上乘算との切り替えを実現にすることができる。

## 【0095】

なお、本実施形態ではキャリー制御機能付き全加算器 42 として図 5 に示すものを用いるようにしたが、キャリー制御機能付き全加算器 42 に代えて、図 6 又は図 7 に示すキャリー制御機能付き全加算器 43 又は 44 を用いるようにしてもよい。

## 【0096】

## 【発明の効果】

以上詳記したように本発明によれば、最小のアーキテクチャを追加するだけで整数型の演算に加えて 2 の拡大体上の演算をも実行できる演算装置及び暗号処理装置を提供することができる。

## 【図面の簡単な説明】

## 【図 1】

本発明の第 1 の実施形態に係る演算装置の構成例を示すブロック図。

## 【図 2】

$c'(x) = a(x) * b(x)$  を実現するための 4 \* 4 ビットの単位乗算の回路構成例を示す図。

## 【図 3】

整数型乗算を実現するための 4 \* 4 ビットの単位乗算の回路構成例を示す図。

## 【図 4】

同実施形態におけるコプロセッサに用いられるキャリー制御機能付きの 4 ビットのリップルキャリー型全加算器の構成例を示すブロック図。

## 【図 5】

同実施形態の加算回路に用いられる全加算器及びキャリー制御スイッチの構成例を示す図。

【図 6】

キャリー制御機能付き全加算器の変形例を示す図。

【図 7】

キャリー制御機能付き全加算器の他の変形例を示す図。

【図 8】

本発明の第 2 の実施形態に係る演算装置の構成例を示すブロック図。

【図 9】

同実施形態の乗算回路を実現するための 4 \* 4 ビットの単位乗算の回路構成例を示す図。

【図 10】

暗号処理用演算用コプロセッサを含む IC カード用 LSI のブロック図。

【図 11】

図 10 に示す LSI におけるコプロセッサ部分の構成例を示すブロック図。

【図 12】

多項式基底の 2 の拡大体演算を行うコプロセッサのハードウェア構成例を示すブロック図。

【図 13】

円分体といわれる 2 の拡大体の乗算回路を示す図。

【符号の説明】

1, 1' ...コプロセッサ

2 ...メモリ

3 ...データバス

1-1 ...整数型乗算回路

1-2 ...2 の拡大体上乘算回路

1-3 ...セレクタ

1-4 ...加算回路

1-5 ...加算回路

1-6 ...キャリー保持部

2-1 ...整数演算制御部

2 2 ... 2 の拡大体演算制御部

3 2 ... 全加算器

3 3 ... スイッチ

4 1 ... 乗算回路

4 2, 4 3, 4 4 ... キャリー制御機能付き全加算器

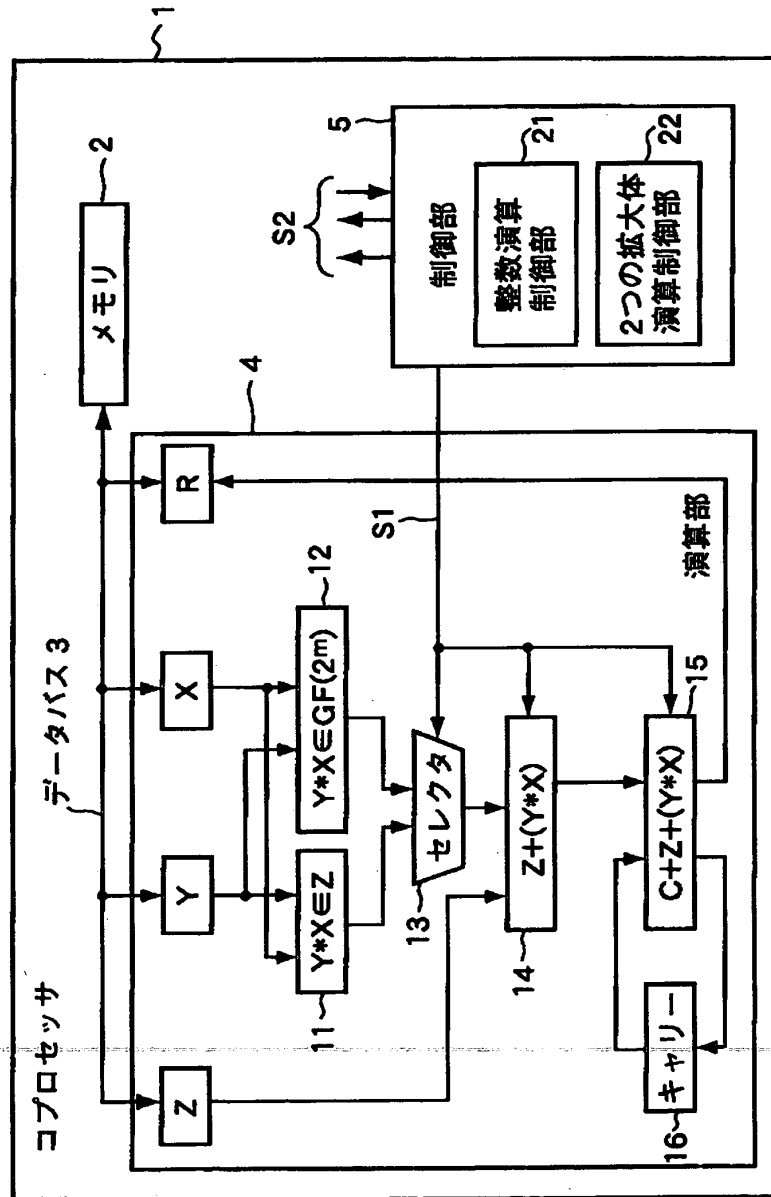
S 1 ... 制御信号



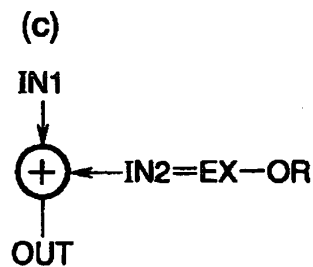
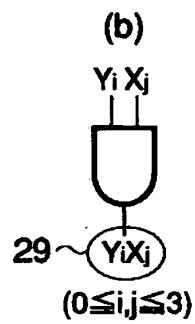
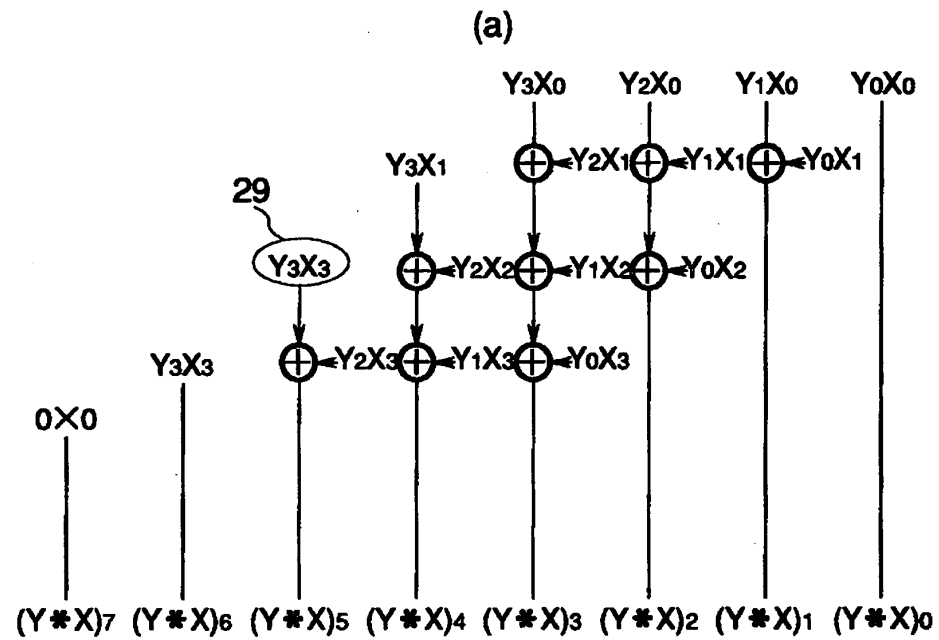
【書類名】

図面

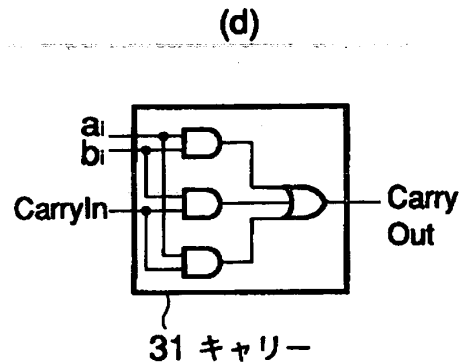
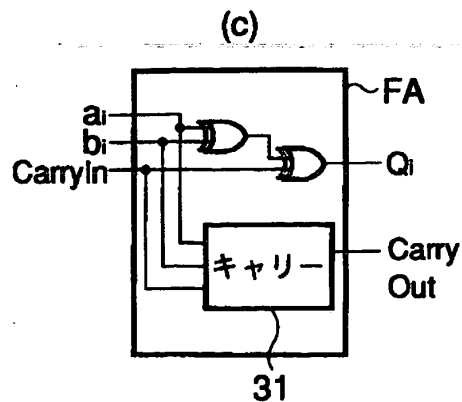
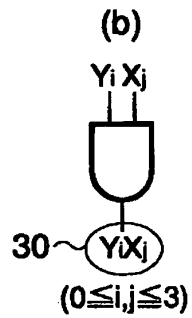
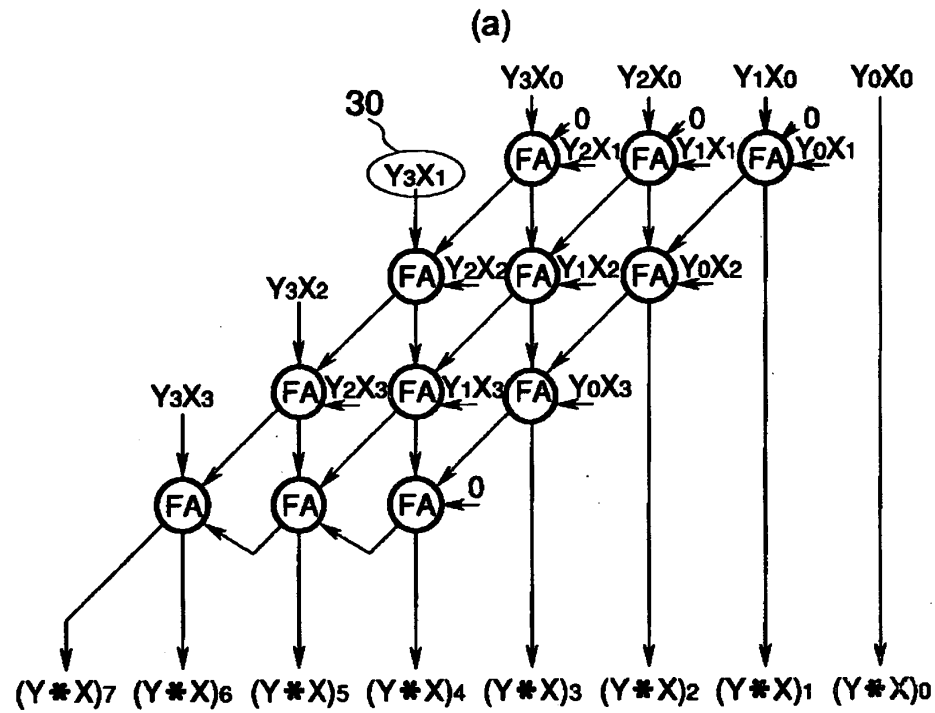
【図1】



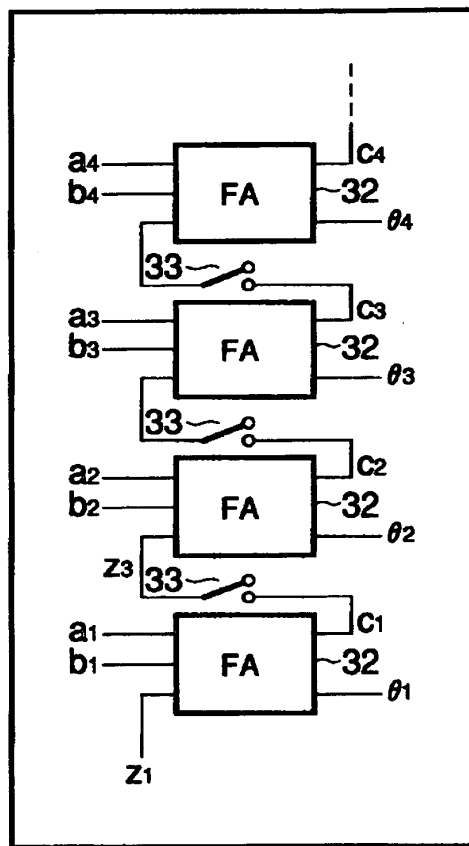
【図 2】



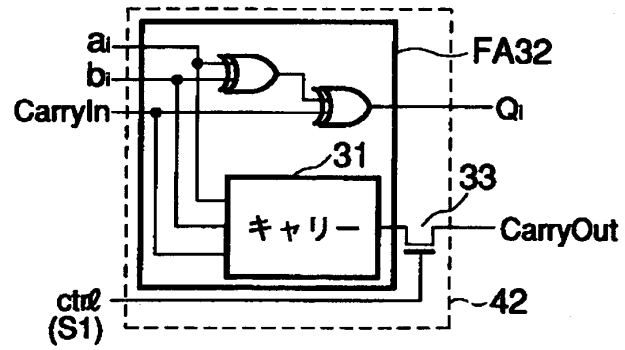
【図 3】



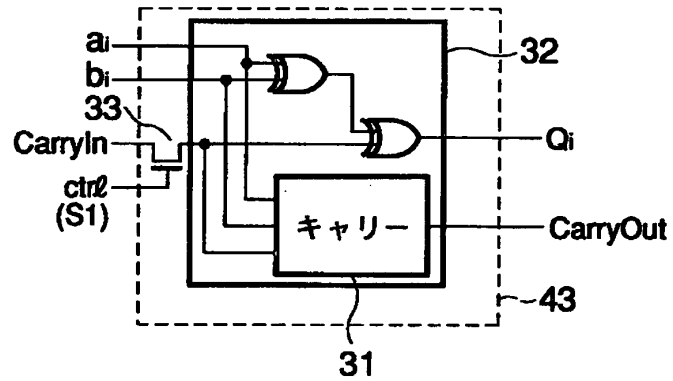
【図 4】



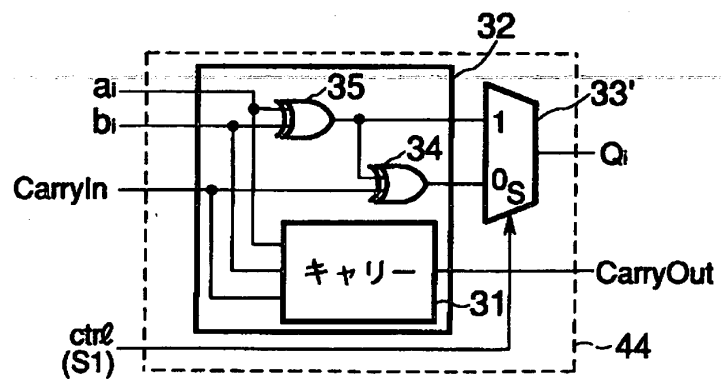
【図 5】



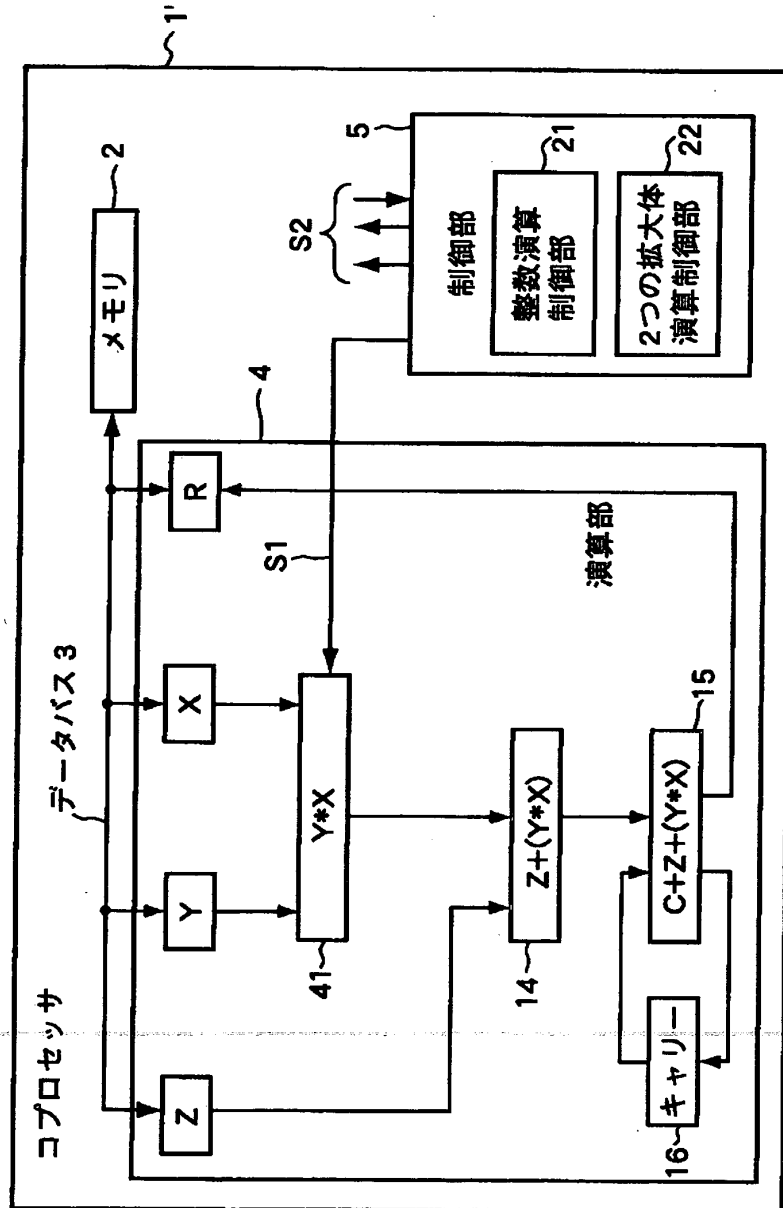
【図 6】



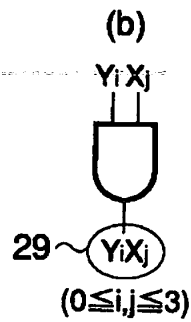
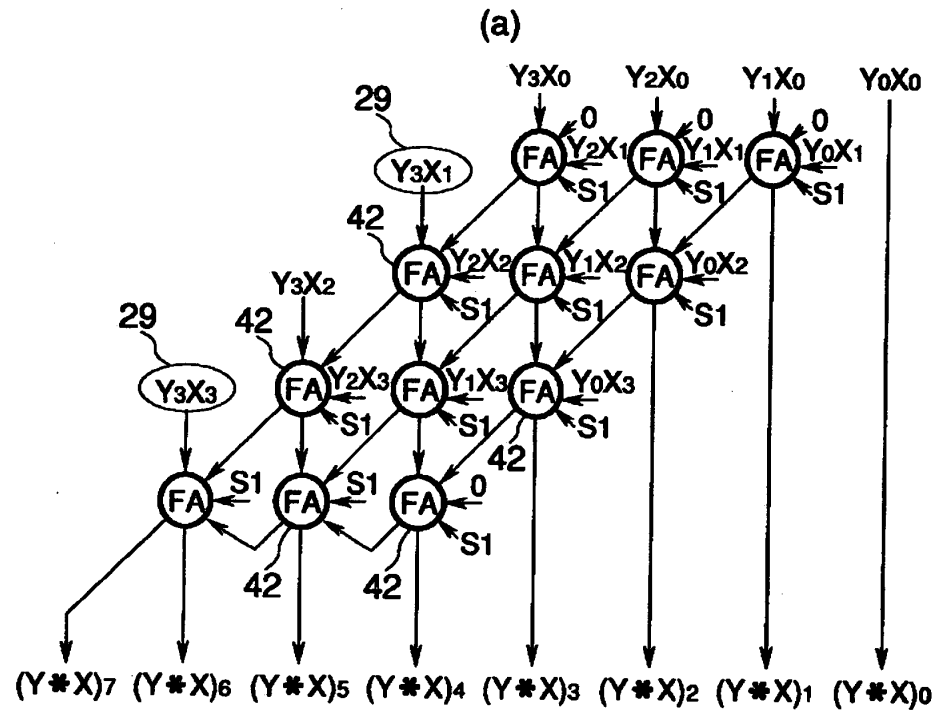
【図 7】



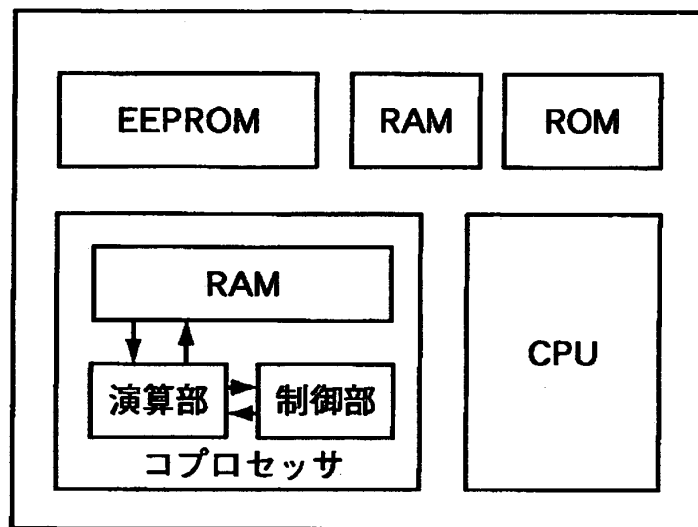
【図8】



【図 9】

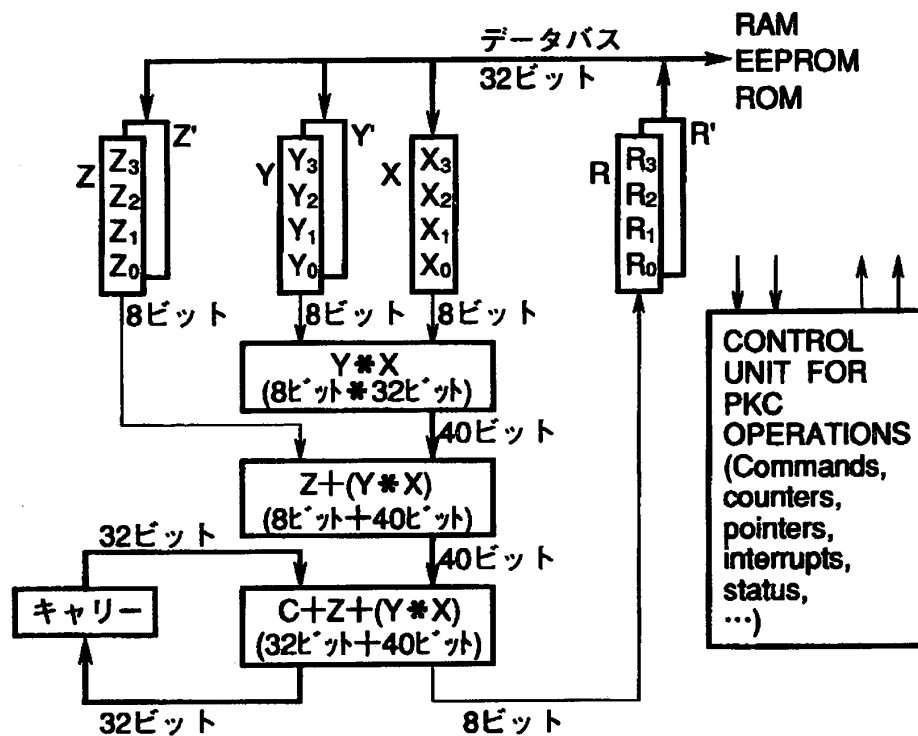


【図 10】

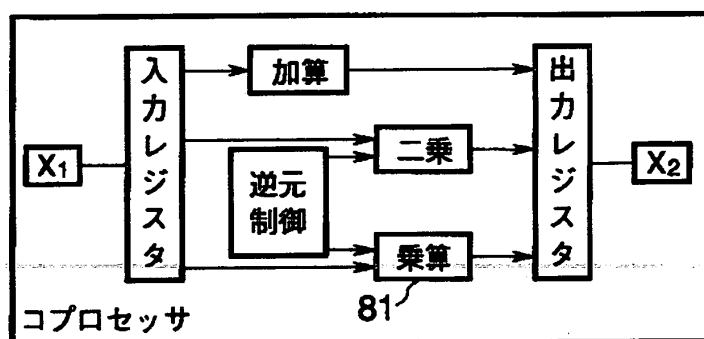




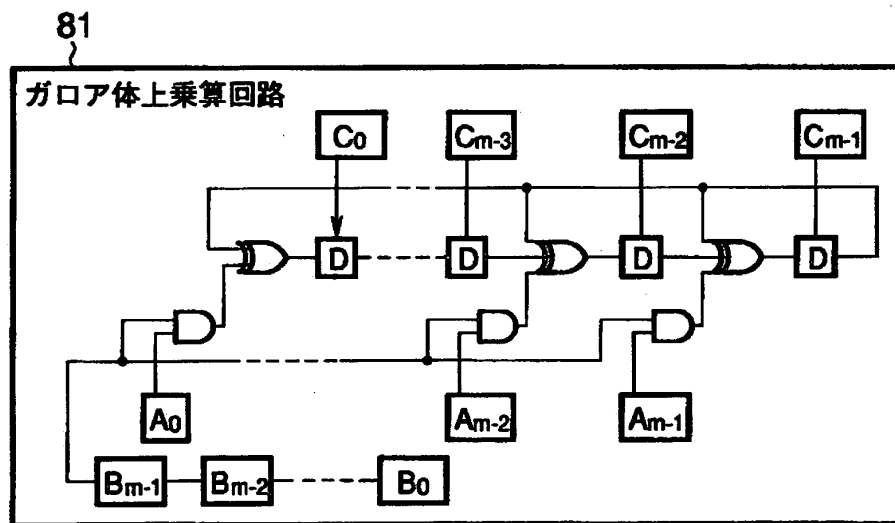
【図 11】



【図 12】



【図 13】



【書類名】 要約書

【要約】

【課題】 本発明は、最小のアーキテクチャを追加するだけで整数型の演算に加えて 2 の拡大体上の演算をも実行できる。

【解決手段】 多倍長の積和演算装置 1 であって、整数型の単位乗算を実行する場合にはキャリーを伝搬させて単位乗算回路 (1 1, 4 1) を動作させ、2 の拡大体の単位乗算を実行する場合にはキャリーを伝搬させずに単位乗算回路 (1 2, 4 1) を動作させるようにした演算装置。

【選択図】 図 1

特平11-011989

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝